AMENDMENT TO THE CLAIMS

1. (Previously Presented) A computer-implemented method of managing data that can be made accessible to a user, comprising:

obtaining a core data set representing a constituent;

obtaining a role-specific data set representing a role assumed by the constituent;

storing the core data set and the role-specific data set so as to distinguish the core data set from the role-specific data set;

obtaining a second role-specific data set representing a second role assumed by the constituent; and

storing the second role-specific data set so as to be separate from said role-specific data set and the core data set.

2. (Original) The method of claim 1, wherein storing comprises storing the core data set and the role-specific data set separate from one another.

3. (Previously Presented) The method of claim 2, wherein obtaining a role-specific data set further comprises obtaining a role-specific data set only containing data that is different than the data stored in the core data set.

4. (canceled)

5. (canceled)

6. (Previously Presented) The method of claim1, wherein obtaining a second role-specific data set comprises obtaining a second role-specific data set only containing data that is different than the data stored in the role-specific and core data sets.

7. (Previously Presented) The method of claim 1, wherein obtaining a role-specific data set representing a role further comprises obtaining a role-specific data set representing a role selected

from the group consisting of customer, supplier, user, employee and contact.

8. (Original) The method of claim 1, further comprising determining whether the user has access to the role-specific data set.

9. (Previously Presented) The method of claim 8, wherein determining whether the user has access comprises filtering user access, based on a characteristic of the user, to a plurality of role-specific data sets including said role-specific data set.

10. (Original) The method of claim 9, wherein filtering user access comprises filtering user access without requiring the user to log-in more than once per session of use.

11. (Original) The method of claim 9, wherein filtering based on a characteristic comprises filtering based on the identity of the user.

12. (Original) The method of claim 9, wherein filtering based on a characteristic comprises filtering based on a role assumed by the user.

13. (Original) The method of claim 9, wherein filtering based on a characteristic comprises filtering based on at least one security rule set by a system administrator.

14. (Original) The method of claim 9, wherein filtering base on a characteristic comprises filtering based on an agency relationship between the user and an organization.

15. (Original) The method of claim 1, further comprising creating an association between the role-specific data set and one or more organizational divisions within an enterprise.

16. (Original) The method of claim 15, further comprising determining, based at least in part on the association, whether the user has access to the role-specific data set.

17. (Currently Amended) The method of claim 16, wherein determining whether the user has access comprises filtering user access, based at least in part on the association, to a plurality of role-specific data sets ~~includeing~~including said role-specific data set.

18. (Original) The method of claim 17, wherein filtering user access comprises filtering user access without requiring the user to log-in more than once per session of use.

19. (Previously Presented) The method of claim 1, wherein obtaining a core data set representing a constituent further comprises obtaining a core data set representing an internal organization constituent.

20. (Previously Presented) The method of claim 1, wherein obtaining a core data set representing a constituent further comprises obtaining a core data set representing an external organization constituent.

21. (Previously Presented) The method of claim 1, wherein obtaining a core data set representing a constituent further comprises obtaining a core data set representing a constituent that is an individual person.

22. (Previously Presented) The method of claim 1, wherein obtaining a core data set representing a constituent further comprises obtaining a core data set having any one of a plurality of specialized formats.

23. (Previously Presented) The method of claim 1, wherein obtaining a role-specific data set representing a role assumed by the constituent comprises obtaining a role-specific data set having a format customized to the role assumed by the constituent.

24. (Previously Presented) A computer-implemented method for distributing access rights, comprising:

receiving a set of log-in information;

identifying, based on the log-in information, a contact record;

identifying an association between an organization record and the contact record, wherein the organization record contains a collection of information related to an organization; and

selectively providing access based at least in part on the association.

25. (Original) The method of claim 24, wherein identifying an association comprises identifying an employment association between an individual affiliated with the contact record and an employer affiliated with the organization record.

26. (Previously Presented) The method of claim 25, wherein selectively providing access further comprises providing access to the organization record when the association indicates the individual is employed by the employer.

27. (Previously Presented) The method of claim 26, wherein selectively providing access further comprises providing access to role-specific records related to the organization record when the association indicates the individual is employed by the employer.

28. (Original) The method of claim 27, wherein providing access to role-specific records comprises selectively providing access to role-specific records based at least in part on a plurality of access security rules.

29. (Original) The method of claim 28, wherein selectively providing access to role-specific records based at least in part on a plurality of access security rules comprises selectively providing access to role-specific records based at least in part on a plurality of access security rules selectively configured by a system administrator.

30. (Previously Presented) The method of claim 28, wherein selectively providing access to role-specific records based at least in part on a plurality of access security rules comprises selectively providing access based at least in part on a plurality of access security rules

distributing access rights based on an identity characteristic of the individual.

31. (Previously Presented) The method of claim 28, wherein selectively providing access to role-specific records based at least in part on a plurality of access security rules comprises selectively providing access based at least in part on a plurality of access security rules distributing access rights based on a role assumed by the individual.

32. (Previously Presented) A system for distributing access rights, the system comprising:

a data management component for receiving data and distributing the data into a plurality of constituent and role-specific records, wherein the data includes information gathered from an interaction with a constituent acting in a first capacity, as well as information gathered from a subsequent interaction with the constituent acting in a capacity different than the first;

a constituent-role association component for maintaining a record of relationships between constituent and role-specific records; and

a security subsystem for distributing access rights based at least in part on the record of relationships.

33. (Original) The system of claim 32, wherein the security subsystem is further configured to distribute access rights based at least in part on a plurality of access security rules.

34. (Original) The system of claim 33, wherein the access security rules are selectively established by a system administrator.

35. (Original) The system of claim 32, wherein:

the record of relationships includes a record of employer-employee relationships; and

the security subsystem is further configured to distribute access rights based at least in part on the record of employer-employee relationships.